

Dr Timothy Noël Peacock - Written evidence (IUD0009)

Dr Timothy Noël Peacock, Lecturer in History & War Studies, Director of UofGGamesLab, University of Glasgow

1) I am submitting evidence based on my ongoing academic research and teaching in History and in the Scottish Centre for War Studies and Conflict Archaeology (into areas including nuclear history, spaceflight and space security, games and wargaming, AI and politics). I am also submitting evidence based on wargaming projects I have led or supported over the past 5 years in my capacity as Director for the c. 300-member Cross-disciplinary Research Lab, UofGGamesLab, at the University of Glasgow.

2) While perhaps most immediately applicable to Q5 on UK Armed Forces updating training and exercises, one potentially valuable measure that is relevant across the different questions would be further supporting development of UK-wide capacity for wargaming and simulation. These games or exercises may, for example, be those conducted by Defence practitioners, Government, businesses, and/or potentially community organisations, at local or national levels as appropriate, whether simpler or more complex physical tabletop or digital games, small or larger-scale exercises that involve in-person/online elements, or a combination. This activity would be to complement other invaluable forms of training and preparation which already occur.

3) Wargames offer one set of means for testing existing plans, developing new ones, and thinking through future possible challenges, and have been used in different contexts relating to the War in Ukraine. Well-executed tabletop exercises, as one example, also offer the potential for rapid iteration of ideas. Research-led wargaming has seen much increased interest and use in recent years, from UK academic, Government and business communities to Defence practitioners and NATO partners, attested to most recently by different speakers at the King's Wargaming Network week-long Conference at KCL in partnership with NATO ACT (16-18 April 2024).

4) While using the term 'wargaming', activities could equally concentrate on challenges that may be the result of war or of other crises, such as threats to critical infrastructure, disruption of supply chains or environmental disasters, all of which have been witnessed in the War in Ukraine, from attacks on power stations to serious flooding caused by the deliberate collapsing of dams.

5) However, as with any educational and training measure, although much valuable work is already being undertaken, there is still significant scope for research and testing into how these tools may be best created, appropriately used, and critically evaluated, to recognise their strengths and their potential limitations.

6) A related step could be looking at what assumptions are made in current or future wargames, whether military or civil, including the extent to which

conditions are assumed, such as wider strategic level considerations of how far logistical difficulties or supply chain disruptions are factored into planning.

7) The War in Ukraine has shown the value of any Defence-related civil planning or wargaming also considering psychological resilience and local involvement – how far communities themselves (whether geographical or organisational) are equipped and motivated to be co-developers of wider resilience planning? One of the single biggest challenges historically to planning, including early Cold War US Civil Defense (among others), were inequalities in implementation, and a lack of community support.

8) While some recent news reporting has raised compulsory military service in different countries, it is not intended to get into that discussion here, except to concur with the Government conclusion of this not being currently appropriate for the UK. However, resulting debates around such service have tended to obscure other forms of valuable resilience planning, training and exercises involving civilian populations in different countries. While often focused on disaster prevention, this type of planning can also be beneficial to Defence preparedness. One challenge of engaging communities in appropriate Defence resilience and civil preparation is how any discourse around non-service-related planning is articulated. It may even be, for instance, that educational gaming serves both as one instructional and also outreach tool in this regard, different games having been used in such areas as public health simulations and education.

9) Relating to Q2 on air and missile defence, part of the calculation for whether there were to be any added investment, and where it should be directed, would include considering the possibilities of adversaries employing threats that may be both higher or (seemingly) lower technology but not at the forefront of current mainstream attention. One example has been the increased use in recent years of uncrewed balloons for surveillance and as decoys to weaken air defences.¹ There has also been discussion of the potential modern use of low-cost GPS-equipped balloons for bombing missions, although the full potential for such usage in the War in Ukraine or beyond remains largely unconfirmed and untested at this stage.²

10) Any consideration of UK air defence would also need to account for psychological or other forms of information-based warfare: possibilities that either smaller or larger numbers of cheaply-manufactured weapons by adversaries would not need successfully to 'attack' targets to be effective, or even be used in attacks at all, but could, nonetheless, by existing, have significant disruptive or psychological effects. Air defence would, as such, need to allow for dealing with wider-scale false reporting, whether accidental or as part of deliberate forms of disinformation and disruption.

¹ Examples including <https://www.bbc.co.uk/news/world-europe-64661145> [16 February 2023].

² <https://www.forbes.com/sites/davidhambling/2024/04/23/ukraine-strikes-russia-with-long-range-bomber-balloons/?sh=6886152477da> [23 April 2024].

11) The large-scale disruption of Gatwick Airport in 2018 over suspected commercial drone sightings, in which no drone or culprit was ever located, offers just one example of how threats could cause significant infrastructure disruption. If coordinated, even a limited number of reported small drone-related threats (whether backed up by actual drones or not) could be magnified through disinformation operations involving news/social media and/or other sources to cause panic and major infrastructure disruptions, without being identified as a conventional, attributable 'attack'.

12) Conversely, in the event of significant aerial attack in which air or missile defences were not sufficient, another aspect relating to Q2 would be the extent to which any such investment is coupled with other developments, including improved survivability of critical Defence and Civil infrastructure, which have been particular targets in Ukraine. One Cold War example from Sweden has been that of enabling the nation's motorways to serve as repurposed air force runways, which included concealed stations for refuelling and re-provisioning, to disperse the air force prior to imminent hostilities to limit damage in the event of bases being rendered inoperative (the Bas 60, later Bas 90 plan). This is not to necessarily suggest such identical provision be made in the UK, but rather to emphasise the importance of ensuring sufficient resilience and engineering redundancy in existing or future infrastructure planning.

13) In thinking about Q4's increasing of the military-industrial base and upskilling the relevant workforce, alongside existing factory processes, it could be helpful further to consider how potential near future developments to manufacturing may either alter or augment these? One notable example may be the further development of 3D printing, a technology which, while still having significant limitations, has been seeing increasing use in the War in Ukraine, including in such areas as production of drone parts and customised drone munitions.³ One of the challenges exposed by the War has been the targeting of production facilities, whether through kinetic strikes or other forms of interference. Comments have already been made in evidence to this Enquiry around the future survivability of soldiers and units partly being based on hiding electronic signals, but could concealment and dispersal end up being applied more widely? For instance, may there be future instances in which some production facilities, instead of being centralised, return to a more widely distributed model in order to ensure resilience against attack? Or even of front-line units able, through being equipped with 3D printers, more easily to build or replace damaged components or systems themselves without relying as heavily on supply lines? The response to such questions would depend on different factors including available defences, strengths or limitations of the technologies involved, and perceived threats.

14) Such technologies as 3D printing also provide the potential, depending on how facilities are developed, for: easier repurposing of their capacity towards peacetime uses; rapidly modifying designs to adapt to new threats;

³ <https://www.forbes.com/sites/davidhambling/2024/04/02/steel-hornets-ukraines-amazon-for-drone-bombs/?sh=1abba029518d> [2 April 2024].

manufacturing (with the right materials) some systems even when supply chains of existing overseas products are disrupted. It may not always be possible, given production specialisation needed for certain procurement, but this added flexibility in 3D printing could be one example of a more cost effective way of achieving re-purposable security infrastructure.

15) This is only to suggest one potential technology – how it could be used as part of an increased military-industrial base would depend on further research and development, including potential wargaming or simulation of strengths and limitations, as well as integration with other systems and appropriate training. 3D printing also presents added challenges which would need to be considered, such as in ensuring cybersecurity of printers themselves. One of the potential added prospects of sabotage could be for invisible faults directly ‘printed’ into systems, where such faults are more difficult to detect than from existing quality assurance processes.

16) Another consideration is that an increased military-industrial base is only as strong as its supply chain. Even where systems are manufactured domestically in the UK, there are (in some instances critical) components or sub-components sourced from overseas suppliers and which cannot, at present, be easily replaced. Recent disruptions to transit of ships through the Red Sea, whether through attacks on shipping or the prior accidental blockage of the Suez Canal in 2021, are just two examples of short-term supply chain fragility. In this regard, it would be valuable further to chart supply chain resilience, and potentially to integrate long-term disruption into such activities as wargaming and exercises of how to manage or mitigate these risks.

17) Such supply chain concerns are also particularly relevant to the earlier air defence question and potential weak points in a conflict, especially given the success of Ukrainian forces in using drones against Russian naval vessels in the Black Sea.

18) There is similarly the consideration of logistical choke points at UK ports. To what extent, for instance, could specialised port facilities required for unloading cargo ships be repaired in the event of disruption? Would there be the need further to plan for the possibility of assembling artificial temporary harbours not only, as they are currently being used, for humanitarian relief in conflict zones internationally, but to ensure continuity of domestic imports in the event of attacks?

19) While different from WW2 U-Boat campaigns in the Battle of the Atlantic, these logistical challenges posed by developments from the War are crucial to consider, given continued UK maritime interests and reliance on sea-based imports. It would be particularly beneficial further to assess protection of merchant shipping from future air, surface, underwater, cyber and political-economic threats, including development and testing of processes through wargames and exercises where appropriate.

20) Any discussion of nuclear diplomacy and escalation relating to the War in Ukraine could be an entire submission in itself, whether relating to new discourses around nuclear blackmail or potential damage to nuclear power stations. At the same time, some of the aforementioned challenges in areas from heightened psychological warfare to logistics, drones and critical infrastructure, all add new dimensions to these nuclear threats and would benefit from further systematic study and simulation.

24 April 2024